Security and Redundancy Whitepaper

Rev. 4/11/2024

DynaFile™ is a web-based document management solution that gives you the tools to improve business. Whether you're looking to consolidate paper files, automate document archiving or integrate an electronic filing system into your current business, DynaFile™ has the versatility and simplicity to allow you to easily go paperless. This document outlines the deliverables, costs and subscription agreement for the application. More information about DynaFile™ can be found by visiting www.dynafile.com.

DynaFile Security & Redundancy

When you subscribe to the DynaFile Document Management System, you entrust us to manage your documents for you and we take that responsibility very seriously. The security and integrity of those documents is of utmost importance to us. Therefore, we have established, developed and continually test security and redundancy of your data on multiple levels.

It is because of the secure and redundant nature of our entire infrastructure that we can guarantee 100% data reliability and security.[1] You will never lose or have a document inadvertently disclosed due to a failure of any part of our infrastructure. This ensures that you will have access to your data 24x7x365 [2] while ensuring that your data is only available to those individuals who should have access to it.

The following items and visual data flow diagram outline the multiple facets of security that are built into each and every DynaFile implementation:

(1) Data Encryption In Flight – All data communicated to and from DynaFile from the user's internet browser is encrypted during transmission utilizing SSL/TLS encryption protocols with a minimum of 2048-bit encryption keys, limited to only the latest and proven secure protocols and ciphers. Each client will have their own unique URL that will be used to access their system and each user must have and use unique authentication credentials to access the system.

(2) Secure File Transmission – Documents scanned from network attached devices can be delivered via secure File Transfer Protocol (FTP). Encryption protocols of FTPS (FTP over SSL) and SFTP (FTP over SSH) are both available. If use those protocols are not available or practical, DynaFile offers a secure, server-based utility, that will transmit scanned documents over an HTTPS connection. To enhance security all FTP communications are "write only" which prevents reading of any data delivered. In addition, the FTP delivery destination is simply a "staging area" for documents which are picked up immediately by the DynaFile application and processed accordingly.

(3) Datacenter Security – All DynaFile servers are housed in SSAE16 certified data centers that have annual AICPA SOC 2 audits performed. This audit procedure ensures compliance with multiple security regulations including PCI, HIPAA, and GLBA. In addition, the DynaFile application and infrastructure has third-party penetration tests performed, at a minimum of monthly, to ensure that unknown vulnerabilities can't be exploited.

(4) Intrusion Prevention – The entire DynaFile infrastructure resides behind multiply redundant Sophos Unified Threat Management firewalls that detect and prevent unauthorized intrusions or attacks. These firewalls not only provide for dynamic real-time intrusion detection and prevention (IDS/IPS) at both the host and network level but can also dynamically adjust configuration parameters and network transmissions in order to prevent continued or future attacks.

(5) Application Redundancy and Isolation – The DynaFile application resides on multiple redundant application servers that reside in an isolated DMZ network zone and are load balanced to scale out as the needs of our clients grow to ensure that your documents will be available 24x7x365 [2].

(6) Security Policies – DynaFile management enforces polices that incorporate the principle of least privilege and segregation, which basically means that your data is logically isolated and separate from other clients or development systems and that only the highest-level security screened individuals or service accounts with absolutely required permissions to maintain or operate the application ever have access your data.

(7) Enterprise Class Infrastructure - All data in DynaFile is stored on enterprise grade flash-based storage area networks (SAN's) with a minimum of Nx2 redundancy for every component in the system. This includes not only the storage, but also all servers, switching networks, firewalls and controllers. This means that we could lose 50% of our entire infrastructure with absolutely no degradation of service. In addition, every piece of hardware and all application functions are monitored continuously with "hot-spares" ready to take over without any manual intervention. It is because of this "over-the-top" redundancy that DynaFile has experienced less than 10 hours of unscheduled unavailability in total in over 10 years of operation!

(8) Database Security – All access to the application is controlled through the database with allows for both user and group level controls. Each client's data is logically separated and isolated in to separate databases. Every document request and any actions available on that document are controlled by explicit permissions, defined by the administrators of the system. All database information is encrypted in real-time and all user credentials are asymmetrically salted and hashed using the key derivation function PBKDF2, standardized in RFC2898, generating keys of 512 bits in length with 272-bit salts, preventing any type of brute-force password attack or extraction mechanisms.

(9) Data Encryption At Rest – In order to comply with compliance regulations and to ensure that your data is never inadvertently disclosed, every document stored in DynaFile is encrypted at rest using governmental FIPS 140-2 certified AES 256-bit encryption in XTS cipher mode. This ensures that even through the normal process of hardware replacement and upgrades, your data will never leave the secure data center in an unencrypted format. In addition, any request for document data is first validated through the database for authorization and then streamed to the user. No individual will ever have raw access to the document information. Finally, each client's data is logically separated and isolated in separate file repositories.

(10) Data Backup – Even though DynaFile's production infrastructure is extremely resilient, backup of the data is still essential in case of a catastrophic failure or, more commonly, inadvertent changes to data caused by user actions. Therefore, all client data and require software infrastructure is backed up using Continuous Data Protection (CDP) methodologies. This means that our backup routines don't have to wait for off-hour backup windows to perform a backup. As soon as document information is added or changed, a replica of that information is automatically sent to our local backup systems and retained for a period of 60 days.

(11) Backup Security – As with the live data stored within DynaFile, all backup (and replication) data is also secured and encrypted using the same security precautions as are used for live data.

(12) Replication and Disaster Recovery – No one likes to think that a natural disaster or an act of terrorism will affect them, but in today's age, these events can happen, and precautions need to be taken to deal with them. Even though DynaFile's primary data center is hardened against almost any unforeseen event, should something happen, and the primary systems become unavailable, you can be assured that your data is still protected. Utilizing real time replication strategies, your data is automatically synchronized with a secondary data center that is geographically separated from the primary. This provides for a Recovery Point Objective (RPO) of less than 60 seconds and a Recovery Time Objective (RTO) of less than 2 hours. This means that should DynaFile's primary data center be completely rendered inoperable, you will still be able to access your information within a matter of hours with little or no loss of information.

If you have further questions about the security, redundancy, disaster recovery or other aspects of the DynaFile system, please feel free to contact us at info@dynafile.com

[1] *Our limit of liability is capped at the minimum of the amount paid for the service over the prior 12-month period or the actual, provable financial loss incurred due to the lost or disclosed data.*

[2] *Uptime guarantees are limited by our Service Level Agreement (SLA) which stipulates that the application will be available to you 99.9% of the time during any given month.*

DynaFile Security Diagram